

House Bill 10
"Long-Range Information Technology Appropriations"
Proponent Testimony by Stuart Fuller
Chief Technology Officer (CTO)
State Information Technology Services Division (SITSD)
Department of Administration
444-1254

Before the
House Long-Range Planning Subcommittee
February 11, 2013

Statewide Data Protection Initiative

The Administration is recommending the Legislature appropriate \$2 million in one-time-only funds to assess the potential risk and mitigate security gaps in the State of Montana's IT systems. This enhancement of existing programs is designed to help prevent hackers from gaining access to Montanan's confidential information.

State and local government entities have been primary targets for the hacker community over the last several years including successful attacks on the State of Utah and Yellowstone County. Targeted attacks have increased significantly over the last 6 months with incidents taking place that affect millions of citizens and cost governments millions of dollars. In October 2012, information including the social security numbers, bank account data, and credit card numbers of 3.6 million taxpayers were stolen when databases in South Carolina Department of Revenue were hacked. A recent report by the South Carolina Office of the Inspector General highlighted the need to have a coordinated approach across state government to help mitigate the risk of data security breaches. A recent national study conducted by Deloitte LLP and NASCIO (National Association of State Chief Information Officers) on Cyber Security in State Governments states "States have a goldmine of medical, financial, other PII (Personally identifiable Information), as well as sensitive business and financial data ". The study goes on to recommend that states do more to assess, communicate, and mitigate security risks.

This request would target the following areas:

Statewide data protection through user access control and verification

DOA/SITSD would implement a statewide data protection system through a user access control and verification system. This type of federated system ties various user login and authorization systems together in a unified whole. Establishing an enterprise data protection system helps address cyber threats by reducing the ability of cyber attackers to gain access to systems. Additional benefits of a data protection system are comprehensive security controls for multiple systems, flexibility in multi-factor authentication, robust auditing capabilities, and the ability to integrate various agency systems together to exchange and manage data. Funding will be used to develop, support, maintain, and operate a statewide data protection system for all state agencies except for the university system.

Statewide data risk assessment and penetration testing

A statewide security risk assessment that includes penetration testing conducted by an external entity specializing in information technology security will be done. This assessment would highlight potential vulnerabilities and generate recommendations to improve security. The assessment is extremely important to agencies which do not have the resources and expertise to conduct an assessment themselves. This effort will also fulfill an IRS (Federal Internal Revenue Service) security requirement for agencies that access federal tax information.

Department of Revenue specific security considerations

The DOR needs to address certain security concerns that are IRS requirements and recommendations as a result of the South Carolina breach. This request includes funding for encryption of tax data and other software to enhance the security of tax records. To address a recommendation from the South Carolina incident, the request includes funding for records management. DOR must oversee the maintenance of the department's paper and electronic records from the time they are created up to their eventual disposal. This effort may include classifying, storing, securing, and destruction of records while maintaining the confidentiality of taxpayer information. Based on a recommendation from the South Carolina incident, this request includes funding for software that will be used to track and store records that is specialized in security and auditing functionality. The request includes scanners to reduce paper records having to be moved between locations.